

GUVERNUL ROMÂNIEI

ORDONANȚĂ DE URGENȚĂ

privind unele măsuri pentru sistemul de guvernanță al Cloud-ului Guvernamental

Având în vedere faptul că tehnologia de Cloud Guvernamental este din ce în ce mai larg adoptată de către autoritățile publice din statele membre ale Uniunii Europene, ca urmare a avantajelor tehnice și economice care privesc procesarea, stocarea datelor și disponibilitatea serviciilor, generând și economii consistente sub aspectul investițiilor și al cheltuielilor operaționale,

Ținând cont de faptul că implementarea proiectului de Cloud Guvernamental este o prioritate asumată de către Guvernul României în Programul de guvernare și în actualul context național și internațional, determinat de pandemia COVID-19, realizarea acestui obiectiv a devenit stringentă, având în vedere că schimbul de date în format electronic în sectorul public este absolut necesar,

Având în vedere că realizarea obiectivului menționat anterior presupune, printre altele, asigurarea unui management unitar și eficient privind gestionarea centralizată a resurselor IT&C, fapt ce impune adoptarea cu celeritate a unor măsuri atât la nivel legislativ, cât și la nivelul gestionării resurselor în condiții de securitate sporită, scalabilitate, flexibilitate și adaptabilitate,

Având în vedere faptul că implementarea Cloud-ului Guvernamental asigură o infrastructură convergentă şi scalabilă, prin omogenizarea şi standardizarea echipamentelor hardware utilizate,

Luând în considerare faptul că prin utilizarea infrastructurii şi serviciilor specifice Cloud-ului Guvernamental se oferă instituţiilor publice o serie de beneficii precum: scalabilitate, flexibilitate, performanţă ridicată, rezilienţă şi siguranţă,

Având în vedere că utilizarea Cloud-ului Guvernamental generează efecte pozitive care se reflectă în plan economic, la nivelul instituţiilor publice, inclusiv rentabilitatea economică, comparativ cu oricare alte sisteme locale sau dedicate, implementate insular, la nivelul fiecărei instituţii în parte,

Deoarece Cloud-ul Guvernamental reprezintă un obiectiv imediat şi urgent în considerarea faptului că implementarea sa asigură utilizarea forței de muncă într-un mod mai eficient, ca urmare a administrării suportului tehnic şi asigurării mentenanţei sistemelor în mod centralizat, fapt ce generează automatizarea pentru managementul elementelor software de la sistemul de operare până la nivel de aplicaţii,

Având în vedere că actualul context pandemic a presupus creşterea gradului de furnizare şi utilizare a serviciilor publice prin mijloacele electronice, iar pentru garantarea desfăşurării proceselor esenţiale funcţionării normale a statului este necesară luarea cu celeritate a măsurilor necesare pentru asigurarea unor mijloace informatice şi de comunicaţii securizate, dar şi adresarea de urgenţă a multitudinii de dificultăţi cu care se confruntă în prezent autorităţile publice în materie de întreţinere a sistemelor informatice actuale, multe dintre acestea fiind dezvoltate în tehnologii vechi şi aflându-se la limita ciclului de viaţă, precum şi lipsa unor mecanisme de autentificare mutuală între sistemele implementate la diferite autorităţi ale statului sau chiar lipsa interoperabilităţii sistemelor informatice,

Luând în considerare iminenţa apariţiei unor disfuncţionalităţi tehnice majore ale unor sisteme de comunicaţii şi tehnologia informaţiei care utilizează tehnologii vechi şi care nu mai beneficiază de suport tehnic oferit de producători sau pentru care nu mai pot fi achiziţionate piese de schimb şi licenţe,

Ținând cont de faptul că întreruperea funcționării acestor sisteme ar afecta furnizarea de servicii esențiale către cetățeni și mediul de afaceri, inclusiv actul de guvernare și capacitatea de intervenție a statului în situații de urgență,

Având în vedere creșterea volumului informațiilor din bazele de date critice administrate de statul român și necesitatea consolidării și interconectării acestora, precum și necesitatea asigurării în mod unitar a securității cibernetice a acestora,

Luând în considerare faptul că una dintre direcțiile de acțiune pentru asigurarea securității naționale prevăzute în Strategia Națională de Apărare a Țării pentru perioada 2020-2024, aprobată prin Hotărârea Parlamentului României nr. 22/2020, este reprezentată de realizarea infrastructurii necesare pentru digitalizarea României, cu scopul eficientizării aparatului administrativ și al creșterii calității serviciilor publice, pentru transpunerea în realitate a acestei direcții de acțiune fiind necesară implementarea proiectului de Cloud Guvernamental,

În considerarea tuturor aspectelor menționate mai sus, dar și a faptului că implementarea Cloud-ului Guvernamental, astfel încât acesta să fie funcțional, necesită parcurgerea unor etape procedurale a căror desfășurare presupune o anumită perioadă de timp, iar orice întârziere în adoptarea de măsuri urgente în acest sens ar crește substanțial riscul de dezangajare a fondurilor europene nerambursabile disponibile în acest moment pentru implementarea Cloud-ului Guvernamental, cu implicații negative asupra fondurilor naționale, reglementarea în regim de urgență a cadrului legal necesar demarării etapelor pentru implementarea acestui proiect este cu atât mai justificată,

Având în vedere totodată existența Strategiei Europene pentru Cloud Computing și aspectele prezentate anterior, se impune intervenția de urgență la nivel legislativ în vederea stabilirii cadrului normativ necesar realizării unei infrastructuri pentru serviciile de Cloud Computing Guvernamental,

În considerarea faptului că toate aceste elemente vizează un interes public și constituie o situație extraordinară, a cărei reglementare nu poate fi amânată și impune adoptarea de măsuri imediate pe calea ordonanței de urgență

În temeiul art. 115 alin. (4) din Constituția României, republicată

Guvernul României adoptă prezenta ordonanță de urgență

Capitolul I
Dispoziții generale

Art. 1 - (1) Prezenta ordonanță de urgență stabilește cadrul general pentru realizarea și administrarea la nivel național a unei infrastructuri de tip cloud intern, implementat și administrat de statul român, denumită Cloud Guvernamental, constând într-un ansamblu de resurse și servicii proprii de tehnologia informației, comunicații și securitate cibernetică, utilizate în comun de entitățile găzduite, reprezentate de autoritățile și instituțiile publice, precum și de structurile aflate în coordonarea, subordonarea și sub autoritatea acestora.

(2) Instituțiile responsabile de realizarea Cloud-ului Guvernamental sunt, Ministerul Cercetării, Inovării și Digitalizării, denumit în continuare MCID, prin Autoritatea pentru Digitalizarea României, denumită în continuare ADR, în colaborare cu Serviciul de Telecomunicații Speciale, denumit în continuare STS și Serviciul Român de Informații, denumit în continuare SRI, conform competențelor stabilite de prezența ordonanță de urgență.

(3) Începând cu data intrării în vigoare a actului normativ prevăzut la art. 3 alin. (1) din prezenta ordonanță de urgență, sistemele informatice utilizate de către autoritățile și instituțiile publice sunt dezvoltate astfel încât să fie pregătite pentru migrarea în Cloud-ul Guvernamental.

(4) Nivelurile agreate ale serviciilor specifice Cloud-ului Guvernamental se stabilesc prin protocol de colaborare încheiat între MCID, ADR, STS și SRI, prin Centrul Național Cyberint, cu respectarea cerințelor prevăzute în actul normativ prevăzut la art. 3 alin. (1).

(5) Activitățile de informare publică cu privire la acțiunile care vizează Cloud-ul Guvernamental se realizează de către MCID, după consultarea ADR, STS și SRI, dacă sunt vizate activitățile din responsabilitatea acestora.

(6) Prezenta ordonanță de urgență nu se aplică sistemelor informatice ale autorităților publice din domeniul apărării, ordinii publice și securității naționale, și nici celor ale autorităților publice prevăzute în Constituție în Titlul III, Capitolele I, II și VI, cu excepția celor care furnizează servicii publice electronice stabilite prin hotărâre a Guvernului.

Art. 2 - În înțelesul prezentei ordonanțe de urgență, următorii termeni se definesc astfel:

a') sistem informatic pregătit pentru migrare în Cloud - sistem informatic a cărui arhitectură și tehnologii folosite pentru realizarea sa permit mutarea și funcționarea în cloud;

b) migrare în cloud - metodologia, procedura și acțiunile necesar a fi realizate prin transferul unui sistem informatic în cloud sau prin reproiectarea tehnologică în cazul sistemelor informatice perimate, fără a altera funcționalitățile existente ale sistemului informatic în cauză;

c) infrastructura de bază a Cloud-ului Guvernamental - clădirile, instalațiile, dotările și echipamentele tehnologice aferente, echipamentele de tehnologia informației și comunicațiilor, inclusiv echipamentele necesare asigurării securității cibernetice, care funcționează în configurații de înaltă disponibilitate, precum și programele software, aplicațiile informatice și licențele asociate acestora;

d) infrastructura ca serviciu (IaaS) - model de punere la dispoziția utilizatorilor, la cererea acestora, pe baza unor drepturi de acces și în limita capacităților disponibile în cloud, într-un mod securizat, a resurselor din infrastructura de bază a Cloud-ului;

e) platforma ca serviciu (PaaS) - model de punere la dispoziția utilizatorilor, la cererea acestora, pe baza unor drepturi de acces și în limita resurselor disponibile în cloud, a unor instrumente de dezvoltare, integrare, management, analiză, securitate și de suport pentru aplicațiile software și datele asociate acestora;

f) software ca serviciu (SaaS) - model de punere la dispoziția utilizatorilor, la cererea acestora, a funcționalităților de utilizare a aplicațiilor furnizorului, care rulează pe o infrastructură cloud computing. Aplicațiile sunt accesibile pe baza unor drepturi de acces, prin diferite dispozitive de tip client, fie prin intermediul unei interfețe de tip thin-client cum ar fi din browser web, fie prin intermediul unei aplicații software dedicate.

g) securitatea cibernetică – totalitatea acțiunilor de prevenire și contracarare a atacurilor cibernetice la nivelul Cloud-ului Guvernamental pe baza unui model partajat de securitate (shared security model) cu responsabilități de partajare a securității între administratorul acestuia (IaaS și PaaS) și entitatea găzduită (SaaS);

h) nivel agreat al serviciilor - set de parametri şi indicatori specifici, în baza cărora este determinată disponibilitatea, performanţa şi calitatea serviciilor oferite;

i) APT - concept utilizat pentru a defini un atac cibernetic derulat de o entitate statală sau grupare ostilă , ce vizează ţinte strategice (din domeniul guvernamental, militar, al securităţii naţionale şi/sau al afacerilor), care, prin intermediul tehnicilor, tacticilor şi procedurilor de nivel ridicat, reuşeşte să fie nedetectabil o perioadă lungă de timp cu scopul de a extrage date pentru a obţine avantaje strategice sau financiare;

j) DDOS - atac cibernetic, din surse multiple, care are ca scop încercare de a perturba funcţionarea normală a unui serviciu sau sistem informatic.

k) serviciu public electronic – serviciu de tip e-guvernare prestat către sectorul public, sectorul privat sau societatea civilă de către o entitate publică sau de către o entitate privată în numele unei entităţi publice, în condiţiile legii, utilizând soluţii oferite de tehnologia informaţiei.

Capitolul II

Atribuţii şi responsabilităţi privind realizarea şi operarea Cloud-ului Guvernamental

Art. 3 - (1) Cerinţele tehnice şi operaţionale privind implementarea, operarea, mentenanţa şi dezvoltarea ulterioară a Cloud-ului Guvernamental, regulile privind stabilirea nivelului agreat de servicii, precum şi cele privind migrarea sistemelor informatice se stabilesc prin hotărâre de guvern, la propunerea MCID împreună cu ADR, cu sprijinul STS şi SRI.

(2) Politicile si Strategia privind implementarea, operarea, utilizarea, mentenanţa şi dezvoltarea ulterioară a Cloud-ului Guvernamental sunt aprobate prin hotărâre de guvern, la propunerea MCID împreună cu ADR.

(3) În îndeplinirea rolului prevăzut la art. 1 alin. (2), MCID are următoarele atribuţii:

a) reprezintă interesele statului român în relaţiile externe privind serviciile de Cloud Guvernamental;

b) stabilește serviciile care vor fi furnizate de Cloud-ul Guvernamental si le promovează în mod corespunzător;

c) stabilește periodicitatea auditurilor prevăzute la art. 10 alin. (4) din prezenta ordonanță de urgență și asigură finanțarea acestora

Art. 4 - (1) ADR stabilește și urmărește punerea în aplicare a strategiei privind implementarea, operarea, mentenanța și dezvoltarea ulterioară a Cloud-ului Guvernamental, inclusiv migrarea și integrarea în Cloud-ul Guvernamental a sistemelor informatice și a serviciilor publice electronice ale instituțiilor și autorităților aparținând administrației publice.

(2) ADR asigură implementarea, administrarea tehnică și operațională, mentenanța, precum și dezvoltarea ulterioară pentru serviciile SaaS specifice Cloud-ului Guvernamental, inclusiv asigurarea, prin acorduri-cadru, conform legislatiei achizitiilor publice, a licențelor specifice serviciilor necesare migrării în Cloud-ul Guvernamental a sistemelor informatice și serviciilor publice electronice.

(3) Migrarea și integrarea în Cloud-ul Guvernamental a sistemelor informatice ale autorităților și instituțiilor publice, precum și cele ale structurilor aflate în coordonarea, subordonarea și sub autoritatea acestora, se asigură de către ADR.

(4) În vederea îndeplinirii prevederilor alin. (1) (3), ADR asigură programele software, aplicațiile informatice și licențele necesare, precum și serviciile de analiză, proiectare și dezvoltare software, după caz.

(5) Finanțarea cheltuielilor pentru activitățile prevăzute la prezentul articol se asigură prin Planul National de Redresare și Reziliență, denumit în continuare PNRR, și de la bugetul de stat sau din alte surse de finanțare, prin bugetul ADR și al altor entități găzduite în Cloud-ul Guvernamental.

Art. 5 - (1) Infrastructura de bază a Cloud-ului Guvernamental este asigurată de STS.

(2) STS asigură implementarea, administrarea tehnică şi operaţională, securitatea cibernetică, mentenanţa, precum şi dezvoltarea ulterioară a serviciilor specifice Cloud-ului Guvernamental, prevăzute la art. 2 lit. c), d) şi e).

(3) STS asigură accesul securizat şi conectivitatea la serviciile specifice Cloud-ului Guvernamental pentru entităţile găzduite.

(4) STS asigură securitatea cibernetică a Cloud-ului Guvernamental prin prevenirea si contracararea atacurilor cibernetice, pentru serviciile prevăzute la art. 2 lit. c), d) şi e), inclusiv a atacurilor de tip DDoS îndreptate împotriva Cloud-ului Guvernamental, în conformitate cu atribuţiile stabilite prin actele normative în vigoare.

(5) STS asigură securitatea cibernetică a serviciilor şi sistemelor informatice proprii din Cloud-ul Guvernamental, prin prevenirea şi contracararea atacurilor cibernetice.

(6) Pentru îndeplinirea rolului prevăzut la alin. (1), STS achiziţionează serviciile de proiectare şi asistenţă tehnică, lucrările de investiţii, inclusiv instalaţiile, dotările şi echipamentele tehnologice aferente clădirii, precum şi echipamentele hardware, programele software, aplicaţiile informatice şi licenţele necesare realizării, dezvoltării ulterioare, mentenanţei şi funcţionării serviciilor prevăzute la art. 2 lit. c), d) şi e) din Cloud-ul Guvernamental.

Art. 6 - (1) SRI asigură securitatea cibernetică a Cloud-ului Guvernamental prin cunoaşterea, prevenirea şi contracararea atacurilor cibernetice, inclusiv a celor complexe, de tip APT, îndreptate împotriva serviciilor specifice Cloud-ului Guvernamental menţionate la art. 2 lit. f) şi a entităţilor găzduite.

(2) SRI, cooperează cu STS, conform competentelor fiecărei instituţii, pentru cunoaşterea, prevenirea şi contracararea atacurilor cibernetice complexe, de tip APT, îndreptate împotriva serviciilor specifice Cloud-ului Guvernamental menţionate la art. 2 lit. d) şi e) prin partajarea evenimentelor de securitate, fără a schimba date de conţinut.

(3) Măsurile prevăzute la alin. (1) şi (2) nu se aplică situaţiilor prevăzute la art. 5 alin. (5).

(4) SRI asigură implementarea, administrarea tehnică şi operaţională, mentenanţa, precum şi dezvoltarea ulterioară a serviciilor de securitate cibernetică ale Cloud-ului Guvernamental, prevăzute la alin. (1) şi (2).

(5) SRI cooperează cu STS, ADR şi entităţile găzduite, în scopul prevenirii atacurilor cibernetice asupra Cloud-ului Guvernamental.

Art. 7 - (1) În cazul sistemelor informatice interconectate cu Cloud-ul Guvernamental care aparţin sistemului naţional de apărare, ordine publică şi securitate naţională, securitatea cibernetică este asigurată şi gestionată de STS şi SRI, în colaborare cu autorităţile şi instituţiile din acest sistem.

(2) În vederea îndeplinirii atribuţiilor prevăzute la art. 5-7, STS şi SRI asigură echipamentele hardware, programele software, aplicaţiile informatice şi licenţele necesare în acest scop, conform competenţelor stabilite prin prezenta ordonanţă.

(3) Finanţarea cheltuielilor pentru activităţile prevăzute de art. 5-7 se asigură prin PNRR şi de la bugetul de stat, potrivit legii, prin bugetele STS şi SRI.

Art. 8 - (1) Entităţile publice ale căror aplicaţii software şi baze de date urmează să migreze în Cloud-ul Guvernamental se stabilesc prin hotărâre de guvern.

(2) Entităţile prevăzute la alin. (1) au obligaţia migrării şi integrării aplicaţiilor software şi bazelor de date în Cloud-ul Guvernamental în termen de 2 ani de la data primirii notificării transmise în acest sens de către ADR, în conformitate cu cerinţele stabilite în hotărârea menţionată la art. 3 alin. (1).

Art. 9 (1) În procesul de dezvoltare, implementare, administrare şi asigurarea securităţii cibernetice a Cloud-ului Guvernamental, instituţiile publice menţionate la art 1 alin (2), , prelucrează date cu caracter personal, în calitate de operatori asociaţi, în conformitate cu responsabilităţile prevăzute la art. 3. – 7. din prezenta ordonanţă de urgenţă, cu respectarea reglementărilor legale aplicabile în domeniul protecţiei datelor cu caracter personal.

(2) Prelucarea datelor cu caracter personal în procesul de utilizare și furnizare a serviciilor publice prin intermediul Cloud-ului Guvernamental se realizează de către entitățile găzduite, cu respectarea reglementărilor legale aplicabile în domeniul protecției datelor cu caracter personal.

(3) Modul și perioada de stocare a datelor cu caracter personal în Cloud-ul Guvernamental, modul de realizare a accesului la aceste date, precum și modul de punere în aplicare a prevederilor art. 12-20 din Regulamentul nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE în raport cu utilizarea și furnizarea serviciilor publice prin intermediul Cloud-ului Guvernamental, se stabilesc prin hotărârea de Guvern menționată la art. 3 alin. (1).

Art. 10 (1) Infrastructura de bază a Cloud-ului Guvernamental, infrastructura ca serviciu (IaaS) si platforma ca serviciu (PaaS), prevăzute la art2. lit.c), d), si e) sunt proprietate publica a statului si in administrarea STS care le achiziționează conform prevederilor legale in vigoare.

(2) Softul aferent migrării în Cloud a soluțiilor informatice și software ca serviciu (SaaS), prevăzute la art 2. lit. b) și f) sunt proprietate publică a statului și în administrarea ADR care le achiziționează conform prevederilor legale in vigoare privind achizițiile publice.

(3) Componentele aferente securității cibernetice prevăzute la art 2. lit. g) sunt proprietate publică a statului și în administrarea STS și SRI care le achiziționează conform competențelor stabilite la art. 5 si 6 din prezenta ordonanță de urgență.

(4) Administratorii serviciilor furnizate la nivel IaaS, PaaS și SaaS vor asigura jurnalizarea evenimentelor și accesului la datele entităților găzduite în Cloud-ul Guvernamental, în scopul realizării de audituri de conformitate periodice pe linia calității, securității și trasabilității datelor, în vederea asigurării transparenței utilizării acestora.

(5) Entitățile găzduite în Cloud-ul Guvernamental pot solicita activități de audit de conformitate pe linia calității, securității și trasabilității pentru datele proprii, finanțate prin bugetul acestora.

(6) Activitățile de audit prevăzute la alin. (4) și (5) sunt realizate de entități externe certificate.

Capitolul III

Dispoziții finale

Art. 11 – (1) Sursa de finanțare a investițiilor, prevazută în PNRR, se asigură prin încheierea unui contract de finanțare între ADR, STS și SRI cu MCID prin Organismul Intermediar pentru Promovarea Societății Informaționale, denumit în continuare OIPSI, din cadrul ADR.

(2) ADR prin OIPSI asigură evaluarea, selecția și semnare a contractului/deciziei de finanțare, monitorizarea tehnică a stadiului de realizare a investiției,.

(3)MCID asigura verificarea și certificarea sumelor solicitate, precum si autorizarea și plataacestora..

(4) Evaluarea, selecția și contractarea investitiei va avea în vedere respectarea etapelor prevăzute în PNRR.

(5) Competența de certificare a îndeplinirii corespunzătoare a condițiilor specifice investiției din PNRR, integrate în cadrul Studiului de Fezabilitate și Proiectului Tehnic și ulterior al documentațiilor de atribuire aparține Comitetului Tehnico-Economic pentru Societatea Informațională, conform Hotărârii Guvernului nr. 941/2013, precum si Comitetului pentru e-guvernare și reducerea birocrației, înființat prin Decizia prim-ministrului nr. 331/2021, în funcție de nivelul de competențe.

(6) În scopul analizei și preavizării Studiului de fezabilitate și Proiectului tehnic prevăzute la alin. (5), la nivelul MCID, prin ordin al ministrului cercetării, inovării și digitalizării, se constituie un grup de experți externi.

(7) Pentru realizarea componentelor Cloud-ului Guvernamental respectiv pentru realizarea IaaS, PaaS, SaaS, securitate cibernetică și migrare a bazelor de date, ADR, STS și SRI organizează dupa caz proceduri de achiziție publică, în conformitate cu legislația în vigoare în domeniul achizițiilor publice .

Art. 12 - Autoritățile și instituțiile publice centrale, precum și structurile aflate în coordonarea, subordonarea și sub autoritatea acestora care furnizează un serviciu public electronic, cu excepția celor prevăzute la art 1 alin (6), au obligația ca în termen de 30 zile de la data solicitării ADR să transmită informațiile de detaliu relevante pentru sistemul/sistemele informatic ce vor fi migrate in Cloud-ul Guvernamental.

Art. 13 - Prevederile art. 6 din Ordonanța de urgență a Guvernului nr. 155/2020 privind unele măsuri pentru elaborarea Planului Național de Redresare și Reziliență al României necesare României pentru accesarea de fonduri externe rambursabile și nerambursabile în cadrul Mecanismului de Redresare și Reziliență, cu modificările și completările ulterioare, se aplică instituțiilor responsabile de realizarea Cloud-ului Guvernamental începând cu data intrării în vigoare a prezentei ordonanțe de urgență.

Art. 14 - În termen de 60 de zile de la intrarea în vigoare a prezentei ordonanțe de urgență, MCID împreună cu ADR, STS și SRI, inițiază hotărârea de guvern prevăzută la art. 3.

PRIM-MINISTRU

NICOLAE-IONEL CIUCĂ